

09818391 #6

BEST AVAILABLE COPY

(translation of the front page of the priority document of
Japanese Patent Application No. 2000-091316)



PATENT OFFICE
JAPANESE GOVERNMENT

RECEIVED
JUL 05 2001
Group 2100

This is to certify that the annexed is a true copy of the
following application as filed with this Office.

Date of Application: March 29, 2000

Application Number : Patent Application 2000-091316

Applicant(s) : Canon Kabushiki Kaisha

April 20, 2001

Commissioner,
Patent Office

Kouzo OIKAWA

Certification Number 2001-3033060



09,818,391

CFO 15244 VS # 2
HY/fu



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 4月25日

出 願 番 号

Application Number:

特願2000-124827

出 願 人

Applicant(s):

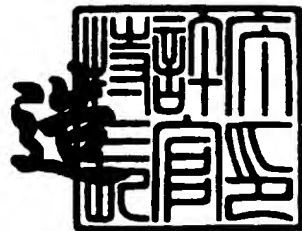
キヤノン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 4月20日

特許庁長官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 4027068

【提出日】 平成12年 4月25日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00

【発明の名称】 ネットワークシステム、リモートアクセス実行装置、方法、及びコンピュータ読み取り可能な記憶媒体

【請求項の数】 34

【発明者】

 【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

 【氏名】 京徳 諭

【特許出願人】

 【識別番号】 000001007

 【氏名又は名称】 キヤノン株式会社

【代理人】

 【識別番号】 100090273

 【弁理士】

 【氏名又は名称】 國分 孝悦

 【電話番号】 03-3590-8901

【手数料の表示】

 【予納台帳番号】 035493

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9705348

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークシステム、リモートアクセス実行装置、方法、及びコンピュータ読み取り可能な記憶媒体

【特許請求の範囲】

【請求項 1】 所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、

上記所定の装置のうち一方の装置は、自機の位置情報を取得する位置情報取得手段と、上記位置情報取得手段により取得された上記位置情報を送信する送信手段を備え、

上記所定の装置のうち他方の装置は、上記送信手段により送信された上記位置情報を受信する受信手段と、上記受信手段により受信された上記位置情報が所定範囲内にあるか否かを照合する照合手段とを備えることを特徴とするネットワークシステム。

【請求項 2】 所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

自機の位置情報を取得する位置情報取得手段と、

上記所定の装置との間のリモートアクセス時に、上記位置情報取得手段により取得された上記位置情報を上記所定の装置に送信する送信手段とを備えたことを特徴とするリモートアクセス実行装置。

【請求項 3】 上記位置情報取得手段は、GPS 受信機により上記位置情報を取得することを特徴とする請求項 2 に記載のリモートアクセス実行装置。

【請求項 4】 所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信手段と、

上記受信手段により受信された上記位置情報が所定範囲内にあるか否かを照合する照合手段とを備えたことを特徴とするリモートアクセス実行装置。

【請求項 5】 上記照合手段により上記位置情報が上記所定範囲内ないと判断された場合、リモートアクセスを切断するリモートアクセス切断手段を備え

たことを特徴とする請求項 4 に記載のリモートアクセス実行装置。

【請求項 6】 上記照合手段は、上記所定の装置との間のリモートアクセス中に繰り返し照合を行うことを特徴とする請求項 4 又は 5 に記載のリモートアクセス実行装置。

【請求項 7】 所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、

上記所定の装置のうち一方の装置は、自機の ID 情報を取得する ID 情報取得手段と、上記 ID 取得手段により取得された上記 ID 情報を送信する送信手段を備え、

上記所定の装置のうち他方の装置は、上記送信手段により送信された上記 ID 情報を受信する受信手段と、上記受信手段により受信された上記 ID 情報による ID が所定 ID であるか否かを照合する照合手段とを備えることを特徴とするネットワークシステム。

【請求項 8】 所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

自機の ID 情報を取得する ID 情報取得手段と、

上記所定の装置との間のリモートアクセス時に、上記 ID 情報取得手段により取得された上記 ID 情報を上記所定の装置に送信する送信手段とを備えたことを特徴とするリモートアクセス実行装置。

【請求項 9】 上記 ID 情報取得手段は、自機の所定個所或いは自機に使用される部材の所定個所に書き込まれた ID を読み取って取得することを特徴とする請求項 8 に記載のリモートアクセス実行装置。

【請求項 10】 半導体製造装置であることを特徴とする請求項 8 に記載のリモートアクセス実行装置。

【請求項 11】 上記 ID はレチクル、レンズ、ウェハ、ステージ、レチクル基準マークのうち少なくともいずれか一に書き込まれていることを特徴とする請求項 10 に記載のリモートアクセス実行装置。

【請求項 12】 上記 ID を光学的に読み取る光学系読み取り手段を備えたことを特徴とする請求項 11 に記載のリモートアクセス実行装置。

【請求項 1 3】 所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の I D 情報を受信する受信手段と、

上記受信手段により受信された上記 I D 情報による I D が所定 I D であるか否かを照合する照合手段とを備えたことを特徴とするリモートアクセス実行装置。

【請求項 1 4】 上記照合手段により上記 I D 情報による I D が上記所定 I D でないと判断された場合、リモートアクセスを切断するリモートアクセス切断手段を備えたことを特徴とする請求項 1 3 に記載のリモートアクセス実行装置。

【請求項 1 5】 上記照合手段は、上記所定の装置との間のリモートアクセス中に繰り返し照合を行うことを特徴とする請求項 1 3 又は 1 4 に記載のリモートアクセス実行装置。

【請求項 1 6】 所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、

上記所定の装置のうち一方の装置は、自機の第 1 の位置情報を取得する位置情報取得手段と、自機の第 2 の位置情報が予め組み合わされている I D 情報を取得する I D 情報取得手段と、上記第 1 の位置情報及び上記 I D 情報を送信する送信手段を備え、

上記所定の装置のうち他方の装置は、上記送信手段により送信された上記第 1 の位置情報及び上記 I D 情報を受信する受信手段と、上記第 1 の位置情報と上記 I D 情報に組み合わされている上記第 2 の位置情報とを照合する照合手段とを備えることを特徴とするネットワークシステム。

【請求項 1 7】 所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

自機の第 1 の位置情報を取得する位置情報取得手段と、

自機の第 2 の位置情報が予め組み合わされている I D 情報を取得する I D 情報取得手段と、

上記所定の装置との間のリモートアクセス時に、上記第 1 の位置情報及び上記 I D 情報を上記所定の装置に送信する送信手段とを備えたことを特徴とするリモ

ートアクセス実行装置。

【請求項 1 8】 上記位置情報取得手段は、GPS 受信機により上記第 1 の位置情報を取得することを特徴とする請求項 1 7 に記載のリモートアクセス実行装置。

【請求項 1 9】 上記 ID 情報取得手段は、自機の所定個所或いは自機に使用される部材の所定個所に書き込まれた ID を読み取って取得することを特徴とする請求項 1 7 に記載のリモートアクセス実行装置。

【請求項 2 0】 所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の第 1 の位置情報、及び上記所定の装置の第 2 の位置情報が予め組み合わされている ID 情報を受信する受信手段と、

上記第 1 の位置情報と上記 ID 情報に組み合わされている上記第 2 の位置情報とを照合する照合手段とを備えたことを特徴とするリモートアクセス実行装置。

【請求項 2 1】 上記照合手段により第 1 の位置情報と上記 ID 情報に組み合わされている上記第 2 の位置情報とが異なると判断された場合、リモートアクセスを切断するリモートアクセス切断手段を備えたことを特徴とする請求項 2 0 に記載のリモートアクセス実行装置。

【請求項 2 2】 上記照合手段は、上記所定の装置との間のリモートアクセス中に繰り返し照合を行うことを特徴とする請求項 2 0 又は 2 1 に記載のリモートアクセス実行装置。

【請求項 2 3】 所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

自機の位置情報を取得する位置情報取得手順と、

上記所定の装置との間のリモートアクセス時に、上記位置情報取得手順により取得された上記位置情報を上記所定の装置に送信する送信手順とを行うことを特徴とするリモートアクセス実行方法。

【請求項 2 4】 所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信処理と、

上記受信処理により受信された上記位置情報が所定範囲内にあるか否かを照合する照合処理とを行うことを特徴とするリモートアクセス実行方法。

【請求項 2 5】 所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

自機の I D 情報を取得する I D 情報取得処理と、

上記所定の装置との間のリモートアクセス時に、上記 I D 情報取得処理により取得された上記 I D 情報を上記所定の装置に送信する送信処理とを行うことを特徴とするリモートアクセス実行方法。

【請求項 2 6】 所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の I D 情報を受信する受信処理と、

上記受信処理により受信された上記 I D 情報による I D が所定 I D であるか否かを照合する照合処理とを行うことを特徴とするリモートアクセス実行方法。

【請求項 2 7】 所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

自機の第 1 の位置情報を取得する位置情報取得処理と、

自機の第 2 の位置情報が予め組み合わされている I D 情報を取得する I D 情報取得処理と、

上記所定の装置との間のリモートアクセス時に、上記第 1 の位置情報及び上記 I D 情報を上記所定の装置に送信する送信処理とを行うことを特徴とするリモートアクセス実行方法。

【請求項 2 8】 所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の第 1 の位置情報、及び上記所定の装置の第 2 の位置情報が予め組み合わされている I D 情報を受信する受信処理と、

上記第 1 の位置情報と上記 I D 情報に組み合わされている上記第 2 の位置情報とを照合する照合処理とを行うことを特徴とするリモートアクセス実行方法。

【請求項 2 9】 所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、

自機の位置情報を取得する位置情報取得手順と、

上記所定の装置との間のリモートアクセス時に、上記位置情報取得手順により取得された上記位置情報を上記所定の装置に送信する送信手順とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項 3 0】 所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信処理と、

上記受信処理により受信された上記位置情報が所定範囲内にあるか否かを照合する照合処理とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項 3 1】 所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、

自機の I D 情報を取得する I D 情報取得処理と、

上記所定の装置との間のリモートアクセス時に、上記 I D 情報取得処理により取得された上記 I D 情報を上記所定の装置に送信する送信処理とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項 3 2】 所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の I D 情報を受信する受信処理と、

上記受信処理により受信された上記 I D 情報による I D が所定 I D であるか否かを照合する照合処理とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項 3 3】 所定の装置との間でリモートアクセスを行うためのプログ

ラムを格納したコンピュータ読み取り可能な記憶媒体であって、

自機の第 1 の位置情報を取得する位置情報取得処理と、

自機の第 2 の位置情報が予め組み合わされている自機の I D 情報を取得する I D 情報取得処理と、

上記所定の装置との間のリモートアクセス時に、上記第 1 の位置情報及び上記 I D 情報を上記所定の装置に送信する送信処理とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項 3 4】 所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、

上記所定の装置との間のリモートアクセス時に、上記所定の装置の第 1 の位置情報、及び上記所定の装置の第 2 の位置情報が予め組み合わされている I D 情報を受信する受信処理と、

上記第 1 の位置情報と上記 I D 情報に組み合わされている上記第 2 の位置情報とを照合する照合処理とを実行するプログラムを格納したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、ネットワークシステム、リモートアクセス実行装置、方法、及びコンピュータ読み取り可能な記憶媒体に関し、特に世界にまたがるネットワーク構築や世界規模で散在する半導体製造工場等において使用される装置のリモート保守管理等のリモートアクセス時における不正アクセスを防止するのに適する。

【 0 0 0 2 】

【従来の技術】

近年、一般のパーソナルコンピュータはもちろんのこと、特定業務向けの装置（半導体製造装置等）、或いはモバイル端末のようなものも、ネットワーク技術の進歩により公衆回線を用いたリモートアクセスが簡単に実現できるようになっている。リモートアクセス技術を用いることにより、例えば、通信回線経由で最新のソフトウェアをダウンロードしてすぐに利用したり、或いは、特定業務向け

の装置であれば24時間の遠隔保守により不具合の調査や修正をサービスマンが赴くことなくタイムリーに実現したり、或いは、装置パラメータの調整をサービスマンが装置設置場所に赴くことなく実現したりする等の、様々な応用が実現可能となっている。

【0003】

ところが、近年、ネットワーク社会の発達、普及に伴って、パスワードの盗用・ハッキングにより、悪意のある第三者がコンピュータネットワークに侵入し、データの改ざんや消去、機密データへのアクセス、顧客情報データの漏洩等の深刻な被害を受ける例が後を絶たないようになってきている。

【0004】

このようなネットワークの不正アクセスによる被害を防止するために、従来から種々の方法が提案されている。例えば、アクセス許可されている電話番号に対してリモートアクセス先から接続しなおすコールバック方式や、アクセス許可電話番号の発信者番号通知を用いて、アクセス許可電話番号のリストに該当するものがない場合には接続不可能とする方式や、リモートアクセスのクライアントとサーバ側とでカウンタ同期方式やANSI規格準拠のチャレンジ・レスポンス方式によりワンタイムパスワード生成器（接続のたびにパスワードを発生させる方式）を用いてアクセス許可を行う方式等がある。

【0005】

【発明が解決しようとする課題】

しかしながら、インターネット等で流通するネットワークハッキング・クラッキング用のソフトウェアは年々高度な技術を持つハッカーの手により強力なものとなってきており、セキュリティの高いといわれてきた方式でも昨今では破られるようになってきている。このため、不正アクセスに対する抜本的な対策を行うために、原理的或いは物理的に絶対にクラッキング不可能な不正アクセス防止方式が提供されることが必要とされている。

【0006】

本発明は、上記のような実情に鑑みてなされたものであり、不正アクセスを確実に防止できるようにすることを目的とする。

【 0 0 0 7 】

【課題を解決するための手段】

本発明のネットワークシステムは、所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、上記所定の装置のうち一方の装置は、自機の位置情報を取得する位置情報取得手段と、上記位置情報取得手段により取得された上記位置情報を送信する送信手段を備え、上記所定の装置のうち他方の装置は、上記送信手段により送信された上記位置情報を受信する受信手段と、上記受信手段により受信された上記位置情報が所定範囲内にあるか否かを照合する照合手段とを備える点に特徴を有する。

【 0 0 0 8 】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、自機の位置情報を取得する位置情報取得手段と、上記所定の装置との間のリモートアクセス時に、上記位置情報取得手段により取得された上記位置情報を上記所定の装置に送信する送信手段とを備えた点に特徴を有する。

【 0 0 0 9 】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信手段と、上記受信手段により受信された上記位置情報が所定範囲内にあるか否かを照合する照合手段とを備えた点に特徴を有する。

【 0 0 1 0 】

また、本発明のネットワークシステムは、所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、上記所定の装置のうち一方の装置は、自機のID情報を取得するID情報取得手段と、上記ID取得手段により取得された上記ID情報を送信する送信手段を備え、上記所定の装置のうち他方の装置は、上記送信手段により送信された上記ID情報を受信する受信手段と、上記受信手段により受信された上記ID情報によるIDが所定IDであるか否かを照合する照合手段とを備える点に特徴を有する。

【 0 0 1 1 】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、自機のID情報を取得するID情報取得手段と、上記所定の装置との間のリモートアクセス時に、上記ID情報取得手段により取得された上記ID情報を上記所定の装置に送信する送信手段とを備えた点に特徴を有する。

【 0 0 1 2 】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置のID情報を受信する受信手段と、上記受信手段により受信された上記ID情報によるIDが所定IDであるか否かを照合する照合手段とを備えた点に特徴を有する。

【 0 0 1 3 】

また、本発明のネットワークシステムは、所定の装置間でのリモートアクセスを可能としたネットワークシステムであって、上記所定の装置のうち一方の装置は、自機の第1の位置情報を取得する位置情報取得手段と、自機の第2の位置情報が予め組み合わされているID情報を取得するID情報取得手段と、上記第1の位置情報及び上記ID情報を送信する送信手段を備え、上記所定の装置のうち他方の装置は、上記送信手段により送信された上記第1の位置情報及び上記ID情報を受信する受信手段と、上記第1の位置情報と上記ID情報に組み合わされている上記第2の位置情報とを照合する照合手段とを備える点に特徴を有する。

【 0 0 1 4 】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、自機の第1の位置情報を取得する位置情報取得手段と、自機の第2の位置情報が予め組み合わされているID情報を取得するID情報取得手段と、上記所定の装置との間のリモートアクセス時に、上記第1の位置情報及び上記ID情報を上記所定の装置に送信する送信手段とを備えた点に特徴を有する。

【 0 0 1 5 】

本発明のリモートアクセス実行装置は、所定の装置との間でリモートアクセスを行うリモートアクセス実行装置であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の第 1 の位置情報、及び上記所定の装置の第 2 の位置情報が予め組み合わされている ID 情報を受信する受信手段と、上記第 1 の位置情報と上記 ID 情報に組み合わされている上記第 2 の位置情報とを照合する照合手段とを備えた点に特徴を有する。

【 0 0 1 6 】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、自機の位置情報を取得する位置情報取得手順と、上記所定の装置との間のリモートアクセス時に、上記位置情報取得手順により取得された上記位置情報を上記所定の装置に送信する送信手順とを行う点に特徴を有する。

【 0 0 1 7 】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信処理と、上記受信処理により受信された上記位置情報が所定範囲内にあるか否かを照合する照合処理とを行う点に特徴を有する。

【 0 0 1 8 】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、自機の ID 情報を取得する ID 情報取得処理と、上記所定の装置との間のリモートアクセス時に、上記 ID 情報取得処理により取得された上記 ID 情報を上記所定の装置に送信する送信処理とを行う点に特徴を有する。

【 0 0 1 9 】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の ID 情報を受信する受信処理と、上記受信処理により受信された上記 ID 情報による ID が所定 ID であるか否かを照合する照合

処理とを行う点に特徴を有する。

【 0 0 2 0 】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、自機の第 1 の位置情報を取得する位置情報取得処理と、自機の第 2 の位置情報が予め組み合わされている ID 情報を取得する ID 情報取得処理と、上記所定の装置との間のリモートアクセス時に、上記第 1 の位置情報及び上記 ID 情報を上記所定の装置に送信する送信処理とを行う点に特徴を有する。

【 0 0 2 1 】

本発明のリモートアクセス実行方法は、所定の装置との間でリモートアクセスを行うリモートアクセス実行方法であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の第 1 の位置情報、及び上記所定の装置の第 2 の位置情報が予め組み合わされている ID 情報を受信する受信処理と、上記第 1 の位置情報と上記 ID 情報に組み合わされている上記第 2 の位置情報とを照合する照合処理とを行う点に特徴を有する。

【 0 0 2 2 】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、自機の位置情報を取得する位置情報取得手順と、上記所定の装置との間のリモートアクセス時に、上記位置情報取得手順により取得された上記位置情報を上記所定の装置に送信する送信手順とを実行するプログラムを格納した点に特徴を有する。

【 0 0 2 3 】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の位置情報を受信する受信処理と、上記受信処理により受信された上記位置情報が所定範囲内にあるか否かを照合する照合処理とを実行するプログラムを格納した点に特徴を有する。

【 0 0 2 4 】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、自機のID情報を取得するID情報取得処理と、上記所定の装置との間のリモートアクセス時に、上記ID情報取得処理により取得された上記ID情報を上記所定の装置に送信する送信処理とを実行するプログラムを格納した点に特徴を有する。

【 0 0 2 5 】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置のID情報を受信する受信処理と、上記受信処理により受信された上記ID情報によるIDが所定IDであるか否かを照合する照合処理とを実行するプログラムを格納した点に特徴を有する。

【 0 0 2 6 】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、自機の第1の位置情報を取得する位置情報取得処理と、自機の第2の位置情報が予め組み合わされている自機のID情報を取得するID情報取得処理と、上記所定の装置との間のリモートアクセス時に、上記第1の位置情報及び上記ID情報を上記所定の装置に送信する送信処理とを実行するプログラムを格納した点に特徴を有する。

【 0 0 2 7 】

本発明のコンピュータ読み取り可能な記憶媒体は、所定の装置との間でリモートアクセスを行うためのプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、上記所定の装置との間のリモートアクセス時に、上記所定の装置の第1の位置情報、及び上記所定の装置の第2の位置情報が予め組み合わされているID情報を受信する受信処理と、上記第1の位置情報と上記ID情報に組み合わされている上記第2の位置情報とを照合する照合処理とを実行するプログラ

ムを格納した点に特徴を有する。

【0028】

【発明の実施の形態】

以下、図面を参照して、本発明のリモートアクセス管理システム、リモートアクセス管理装置、方法、及びコンピュータ読み取り可能な記憶媒体の実施の形態について説明する。本実施の形態では、本発明を適用する例として、地理的に離れた拠点に設置される装置として、ステッパー（光縮小投影露光装置）等の半導体露光装置について説明する。そして、サーバ機150等との間でリモートアクセスを行うことにより、リモート保守等のサービスが実現されるようにしている。

【0029】

（第1の実施の形態）

図1には、半導体露光装置のハードウェアシステム構成を示す。101はコンソール用CPUであり、半導体露光装置のコンソール表示とコンソールコマンド入力による操作の制御を司る。102はRAMであり、CPU101が実行プログラムを格納したりデータを格納したりする。103はROMであり、プログラムを格納する。

【0030】

104は補助記憶装置であり、データ及びプログラムを格納するために用いられる。通常、ソフトウェアプログラムは、この補助記憶装置104に保存される。ソフトウェアプログラムは、一般にファイルシステムを補助記憶装置104上に構成しファイルとして管理する。補助記憶装置104としては、ハードディスク等の磁気ディスク装置を用いることが多いが、装置構成や露光作業の性質、運用の違いに応じて、フラッシュメモリやNV-RAM（不揮発性メモリ）、EEP-ROMといったソフトウェア的な書き換え可能な部品を用いることもある。

【0031】

106はGPS用インターフェースであり、後述するGPS受信機108と通信を行う。GPS用インターフェース106としては、一般にRS232C等のシリアル通信インターフェースを用いることが多いが、GPS通信におけるデー

タ量によってはパラレルインターフェースやSCSIインターフェース等を用いてもかまわない。また、GPS用インターフェース106とGPS受信機108との間で行う通信のプロトコルとして、一般に無手順非同期方式を用いるが、同期式やバイナリ手順を採用してもかまわない。

【0032】

105はコンソール装置であり、オペレータ（操作者）は本装置105よりコンソール用CPU101に対する指令を行うことができる。コンソール装置105の表示装置としては、CRTや液晶表示装置、ELパネル、或いはプラズマディスプレイ等を用いる。また、コンソール装置105の入力装置としては、コマンドをキー入力するためのキーボードを用いることが多いが、電子ペンによるペン入力装置（タブレット）やタッチパネル等で構成されることもある。

【0033】

108はGPS（Global Positioning System）受信機であり、衛星からのGPS電波を受信するためのGPSアンテナからGPS電波内のデジタル信号を復号（デコード）し、半導体露光装置が設置されている緯度経度情報（位置情報）や時刻情報を取得する。GPSアンテナは、装置がクリーンルーム等の電波の届かない所にある場合、電波の届く外部まで電線を延長して敷設することも可能である。

【0034】

109は通信インターフェースであり、外部通信網（公衆電話回線網等）と通信を行う通信装置116と通信を行ってリモートアクセスを実現する。通信インターフェース109としては、一般にRS232C等のシリアル通信インターフェースを用いる場合が多いが、パラレルインターフェースやUSB等の高速インターフェースを用いることも多くなっている。

【0035】

116は通信装置であり、公衆回線等の通信網117を用いて遠隔の装置（サーバ機150等）とのリモートアクセスを実現する。通信装置116としては、通信網117がアナログ公衆回線等の場合にはモデム等の装置を用いるが、通信網117がISDN等のデジタル公衆回線等であったり、デジタル専用線で

あったりする場合にはデジタル通信用のターミナルアダプタ（TA）等を用いる。或いは、PHSや携帯電話用のデジタル通信であれば、PHSや携帯電話用のデジタル通信カードを用いることもある。

【0036】

上記通信インターフェース109及び通信装置116を用いてリモートアクセスを可能とするための通信プロトコルには、一般にTCP/IPによるポイント・トゥー・ポイント接続（PPP接続）等を用いるが、リモートアクセスを実現できるプロトコルであれば、アップルトークやネットウェア、或いはパソコン通信等で用いられるベーシック手順等を用いて実現してもかまわない。

【0037】

110はメインCPUであり、半導体露光装置を構成する各種の制御装置を全体制御する。当該メインCPU110と上記コンソール用CPU101とは、メインCPUバス107により接続され、半導体露光装置として動作する。

【0038】

111は照明装置であり、半導体製造用のウェハに対して露光する光源を制御するためのものである。112はレチクル駆動装置であり、半導体製造用のウェハに対して露光するパターンを描いたレチクル（フォトマスク）の搬入搬出等を制御するためのものである。113はステージ駆動装置であり、半導体製造用のウェハをステップアンドリピートの方式で露光するためにXYステージ上でウェハを駆動制御するためのものである。114はアライメント用TVシステムであり、半導体製造用のウェハの正確な位置決めをして制御するためのものである。これら各装置111～114は、周辺機器用バス115によりメインCPU110の制御下におかれる。本実施の形態では、周辺機器用バス115としてSCIを用いるが、どのような汎用の標準バスで構成されていてもかまわない。

【0039】

次に、図2のフローチャートに基づいて、第1の実施の形態における不正アクセス防止のための処理動作について説明する。前提として、リモートアクセスを許可したユーザからは、当該ユーザの半導体露光装置の設置場所の緯度経度情報を予め取得しておく。そして、半導体露光装置との間でリモートアクセスを行う

サーバ機 1 5 0 等には、上記予め取得した半導体露光装置の設置場所の緯度経度情報と、許容される緯度経度のオフセット範囲（どれくらいの距離の移動を許容するかという範囲）の情報とのリストを記憶させておく。

【 0 0 4 0 】

図 2 のフローチャートに示すプログラムルーチンは、半導体露光装置とサーバ機 1 5 0 等との間でのリモートアクセスが開始されると実行され、また、リモートアクセス中に一定の基準で何度も繰り返し実行される。

【 0 0 4 1 】

半導体露光装置では、半導体露光装置に埋め込まれている G P S 受信機 1 0 8 により、当該半導体露光装置が現在設置されている場所の緯度経度情報が取得される（ステップ 2 0 1）。そして、この G P S 受信データ（緯度経度情報）は、通信インターフェース 1 0 9 及び通信装置 1 1 6 を介してリモートアクセスの相手であるサーバ機 1 5 0 等へ送出される（ステップ 2 0 2）。

【 0 0 4 2 】

サーバ機 1 5 0 等では、半導体露光装置から上記 G P S 受信データを受信して、その G P S 受信データによる装置設置場所の緯度経度情報を、許容される緯度経度のオフセット範囲を加算して算出したリモートアクセスを許可すべきユーザ装置設置場所の緯度経度情報と比較・照合する（ステップ 2 0 3）。そして、上記比較・照合した結果、上記 G P S 受信データによる装置設置場所の緯度経度情報がオフセット範囲からずれているような場合には、不正な設置場所データ、或いは改ざん、偽造による無効な G P S 受信データであると判断し（ステップ 2 0 4）、ステップ 2 0 5 に移行してリモートアクセスを切断する。

【 0 0 4 3 】

以上述べた動作により、リモートアクセスを許可した半導体露光装置の設置場所以外の場所からの不正アクセスを防止することができる。特に、半導体露光装置等では、リモートアクセスが全世界的に配置されている拠点間のリモート保守等のネットワーク接続に利用される場合が多いので、本実施の形態における不正リモートアクセス防止方式は有効である。なお、実際の運用においては、本実施の形態で述べた方式と、従来の方式、例えばコールバック方式、着信電話番号を

照合する方式、或いはワンタイムパスワード方式等を併用してもよい。

【 0 0 4 4 】

(第 2 の実施の形態)

上記第 1 の実施の形態では、GPS 受信機 1 0 8 により取得した半導体露光装置の緯度経度情報を送信することにより不正アクセスを防止するようにしたが、本第 2 の実施の形態では、半導体露光装置の光学系部品或いは媒体に書き込まれた装置固有の ID を送信することにより不正アクセスを防止する。

【 0 0 4 5 】

第 2 の実施の形態における半導体露光装置のハードウェアシステムの基本的な構成は、図 1 で説明したのと同様であるが、GPS 受信機 1 0 8 や GPS 用インターフェース 1 0 6 は必要ではなく、装置固有の ID を読み取るための ID 読み取り手段が必要となる。

【 0 0 4 6 】

半導体露光装置では、メイン CPU 1 1 0 からの指示によって、照明装置 1 1 1 等を動作させ、各装置、例えばレチクル駆動装置 1 1 2 であれば、レチクルに書き込まれた装置固有の ID を読み取って、周辺機器用バス 1 1 5 に当該 ID のデータを送出し、メイン CPU 1 1 0 へ ID のデータを受け渡す。

【 0 0 4 7 】

上記 ID のデータはメイン CPU 1 1 0 から RAM 1 0 2 に書き込まれ、コンソール用 CPU 1 0 1 の指令により通信インターフェース 1 0 9 及び通信装置 1 1 6 に渡されて、通信網 1 1 7 を介してリモートアクセスの相手であるサーバ機 1 5 0 等へ送出される。上記 ID のデータは、例えば ASCII テキストのようなデータであってもよいが、レチクルに書き込む際になんらかの暗号化を施しておき、上記暗号化されているデータのまま送出し、リモートアクセスの相手であるサーバ機 1 5 0 等で管理されている秘密鍵を用いて復号するような実施の形態が望ましい。

【 0 0 4 8 】

図 3 には、半導体露光装置の模式図を示す。図 3 において、3 0 1 は照明装置 1 1 1 の露光光源、3 0 2 は露光量制御のためのシャッタ、3 0 3 は回路パター

ンの原板となるレチクル、304はレチクル303を保持するためのレチクルステージ、305はレチクル303を搬入するためのレチクルハンドである。

【0049】

また、306は投影レンズ、307は半導体基盤であるウェハ、308はウェハ307を保持し、露光光源301とのフォーカスを合わせるためのウェハZステージ、309はウェハZステージ308をXY方向へ移動させるためのXYステージ、310はXYステージ309の位置を計測するためのレーザ干渉計、311は露光処理をするためのウェハ307をウェハZステージ308へ供給するためのウェハ供給ハンド、312は露光処理を終えたウェハ307をウェハZステージ308から回収するためのウェハ回収ハンドである。

【0050】

図3に示した半導体露光装置等の光学機器には、レチクル303やレチクルステージ304、或いはウェハZステージ308やXYステージ309といった特殊な部品を具備している。レチクル303やステージ304、308、309等には、レチクルやウェハの位置合わせを行うためのレチクルセットマークやレチクル基準マーク、ステージ基準マーク、TTL-AF基準マーク或いはウェハ基準マークといったマイクロメータ単位の微小なパターンマーク図形が書き込まれており、これらパターンやマークの読み取りには微小パターンを読み取るための各種の特殊な光学系スコープを用いる。

【0051】

本実施の形態では、上記パターンやマークとして、装置固有のIDをテストレチクルやテストウェハ、或いは半永久的に交換する可能性のないステージ等に微小パターンとして書き込み、当該IDを上記光学系スコープにより読み取る手段を具備することによってIDを生成する。

【0052】

IDを生成するのに特殊な光学系デバイスと光学系読み取り装置とを必要とし、かつ上記読み取り手段をリモートアクセス時に必ず実行しなければIDを取得できない構成となるため、IDの偽造や改ざん、或いはIDの読み取り手段のバイパスによる不正アクセスに対して強力な防衛手段となる。

【 0 0 5 3 】

レチクル等の光学部品に書き込まれた文字パターン等のデータは、上記光学系スコープにより読み取ったデジタル画像から文字認識を行い、文字データとして取得するのが望ましい。上記文字データは、装置の製造シリアル番号等をそのまま A S C I I コード等で記述したものを I D として利用してもよいが、装置の製造シリアル番号等を秘密鍵によって暗号化した文字データをレチクル等の特殊光学系部品に書き込み、上記暗号化された I D の復号は、リモートアクセスの相手であるサーバ機 1 5 0 等の上で管理されている秘密鍵を用いて復号し、リモートアクセスの許可されている I D のリストとの照合を行う構成とすることが望ましい。

【 0 0 5 4 】

次に、図 4 のフローチャートに基づいて、第 2 の実施の形態における不正アクセス防止のための処理動作について説明する。前提として、半導体露光装置との間でリモートアクセスを行うサーバ機 1 5 0 等には、リモートアクセスを許可する I D のリストを記憶させておく。

【 0 0 5 5 】

図 4 のフローチャートに示すプログラムルーチンは、半導体露光装置とサーバ機 1 5 0 等との間でのリモートアクセスが開始されると実行され、また、リモートアクセス中に一定の基準で何度も繰り返し実行される。

【 0 0 5 6 】

半導体露光装置では、レチクル等の特殊な光学系部品に書き込まれた装置固有の I D が取得される（ステップ 4 0 1）。そして、この I D のデータは、通信インターフェース 1 0 9 及び通信装置 1 1 6 を介してリモートアクセスの相手であるサーバ機 1 5 0 等へ送出される（ステップ 4 0 2）。

【 0 0 5 7 】

サーバ機 1 5 0 等では、半導体露光装置から上記 I D のデータを受信して、その I D が、リモートアクセスを許可する I D のリストにあるか否かを比較・照合する（ステップ 4 0 3）。そして、上記比較・照合した結果、リストにないような場合には、不正な I D であると判断し（ステップ 4 0 4）、ステップ 4 0 5 に

移行してリモートアクセスを切断する。

【 0 0 5 8 】

以上述べた動作により、リモートアクセスを許可した I D を取得できない半導体露光装置からの不正アクセスを防止することができる。I D を特殊な光学系部品からスコープ等の特殊な光学系装置で読み取る手段は、リモートアクセス中に、一定の基準で随時行われるようにリモートアクセス用のプログラム内に埋め込まれている。すなわち、リモートアクセス用のプログラム動作中は、必ず読み取り手段が動作して I D を読み取るので、本実施の形態における不正アクセス防止方式を回避してリモートアクセスすることは非常に困難であるといえる。

【 0 0 5 9 】

また、上述したように、リモートアクセスの相手であるサーバ機 1 5 0 等で管理している秘密鍵を用いて暗号化した I D をレチクル等の特殊な光学系部品に書き込むようにすることで、通信プロトコル上に送出される I D は暗号化されたものとなり、セキュリティレベルの向上を図ることが可能となる。

【 0 0 6 0 】

従来は、装置固有の I D や前述のワンタイムパスワード方式の秘密鍵の保持方式としては、半導体で作られた記憶素子（メモリ）に書き込んで保持するものであったが、本実施の形態では、物理的、光学的に特殊な特性を有する部品或いは媒体に I D や秘密鍵等を書き込み、それを光学的に読み取るようにしたので、高度な技術を持つハッカーでも I D 等の偽造が原理的に困難であり、不正アクセスを有効に防止することが可能となる。

【 0 0 6 1 】

（第 3 の実施の形態）

第 3 の実施の形態では、上記第 1 の実施の形態で説明したように G P S 受信機 1 0 8 により取得した緯度経度情報と、上記第 2 の実施の形態で説明したように半導体露光装置の光学系部品或いは媒体に書き込まれた装置固有の I D とを、リモートアクセスの相手であるサーバ機 1 5 0 等に送信することにより不正アクセスを防止するようにしている。さらに、I D として、装置設置場所情報を組み合わせた複合 I D を用いることにより、多段階の不正アクセス防止方式を提供する

ことができ、より確実に不正アクセスを防止することができる。

【 0 0 6 2 】

図 5 のフローチャートに基づいて、第 3 の実施の形態における不正アクセス防止のための処理動作について説明する。図 5 のフローチャートに示すプログラムルーチンは、半導体露光装置とサーバ機 1 5 0 等との間でのリモートアクセスが開始されると実行され、また、リモートアクセス中に一定の基準で何度も繰り返し実行される。

【 0 0 6 3 】

半導体露光装置では、半導体露光装置に埋め込まれている G P S 受信機 1 0 8 により、当該半導体露光装置が現在設置されている場所の緯度経度情報が取得される（ステップ 5 0 1）。また、レチクル等の特殊な光学系部品に書き込まれた装置固有の製造シリアル番号等と装置設置場所情報を組み合わせた複合 I D が取得される（ステップ 5 0 2）。そして、G P S 受信データ（緯度経度情報）と複合 I D のデータとは、通信インターフェース 1 0 9 及び通信装置 1 1 6 を介してリモートアクセスの相手であるサーバ機 1 5 0 等へ送出される（ステップ 5 0 3）。

【 0 0 6 4 】

サーバ機 1 5 0 等では、半導体露光装置からの上記 G P S 受信データ及び上記複合 I D のデータを受信して、その G P S 受信データによる装置設置場所の緯度経度情報を、許容される緯度経度のオフセット範囲を加算して算出したリモートアクセスを許可すべきユーザ装置設置場所の緯度経度情報と比較・照合する（ステップ 5 0 4）。また、その複合 I D が、リモートアクセスを許可する I D のリストにあるか否かを比較・照合する（ステップ 5 0 6）。

【 0 0 6 5 】

そして、上記比較・照合した結果、半導体露光装置の現在設置されている場所の緯度経度情報がオフセット範囲からずれているような場合には、不正な設置場所データ、或いは改ざん、偽造による無効な G P S 受信データであると判断し（ステップ 5 0 8）、ステップ 5 1 1 に移行してリモートアクセスを切断する。同様に、リモートアクセスを許可する I D のリストにないような場合には、不正な

I Dであると判断し（ステップ509）、ステップ511に移行してリモートアクセスを切断する。さらに、上記複合I D上の装置設置場所情報と、上記GPS受信データによる緯度経度情報とに相違があれば（ステップ510）、ステップ511に移行してリモートアクセスを切断する。

【0066】

以上述べた動作により、上記第1、2の実施の形態で述べた効果が得られるとともに、I Dとして、装置設置場所情報を組み合わせた複合I Dを用いることにより、多段階の不正アクセス防止方式を提供することができ、より確実に不正アクセスを防止することができる。

【0067】

なお、図1に示したGPS受信機108と装置とのインターフェースを装置の内部に埋め込むことなく、LAN等のネットワークによる通信網を介して、GPS受信機108よりのデータを送信する実施の形態も実現可能である。例えば、半導体露光装置がクリーンルームに設置されており、装置に埋め込まれたGPS受信機からアンテナをGPS電波の受信可能な場所まで敷設することが困難な場合に効果的である。

【0068】

ただし、本方式ではネットワークとの通信インターフェースがGPS受信機108と装置との間に介在するため、ネットワークパケット内容の改ざんや暗号の解読により、本方式による違法コピー防止方式が破られてしまうおそれがある。最も強力な実施の形態は、装置内部にGPS受信機108と装置との切り離し不可能なインターフェースを確保する形態である。

【0069】

（その他の実施の形態）

上述した実施の形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置或いはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステム或いは装置のコンピュータ（CPU或いはMPU）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも

、本発明の範疇に含まれる。

【0070】

また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性のメモリカード、ROM等を用いることができる。

【0071】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているOS（オペレーティングシステム）或いは他のアプリケーションソフト等と共同して上述の実施の形態の機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることはいうまでもない。

【0072】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部又は全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれることはいうまでもない。

【0073】

なお、上記実施の形態において示した各部の形状及び構造は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

【0074】

【発明の効果】

以上述べたように本発明によれば、リモートアクセスを許可した装置設置場所以外からのリモートアクセスや、リモートアクセスを許可するIDを持たない装置からのリモートアクセスを発見することができ、不正アクセスを防止することが可能となる。

【図面の簡単な説明】

【図1】

半導体露光装置のハードウェア構成を示す図である。

【図2】

第1の実施の形態における処理動作を示すフローチャートである。

【図3】

半導体露光装置の模式図である。

【図4】

第2の実施の形態における処理動作を示すフローチャートである。

【図5】

第3の実施の形態における処理動作を示すフローチャートである。

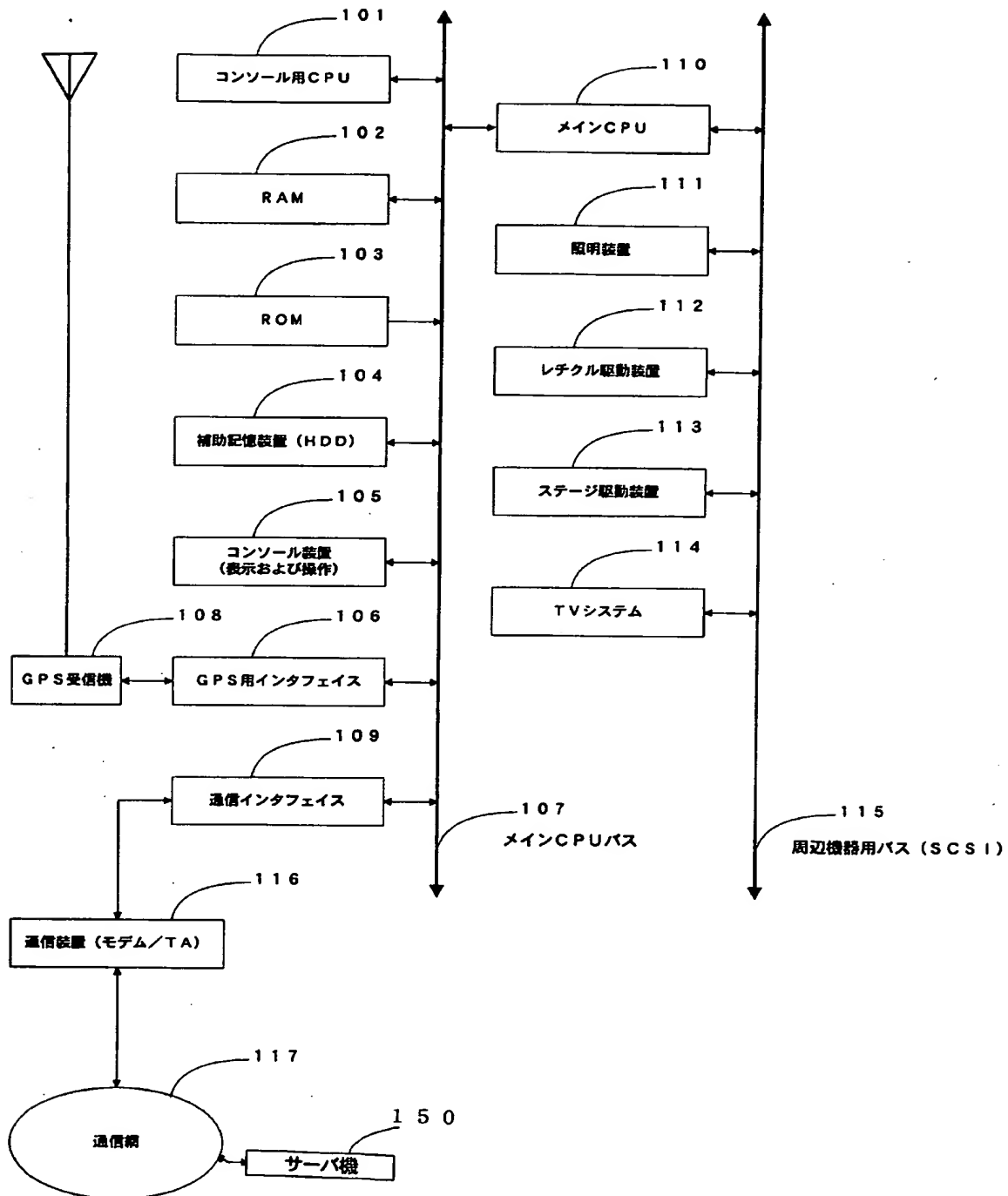
【符号の説明】

- 101 コンソール用CPU
- 102 RAM
- 103 ROM
- 104 補助記憶装置
- 105 コンソール装置
- 106 GPS用インターフェース
- 107 メインCPUバス
- 108 GPS受信機
- 109 通信インターフェース
- 110 メインCPU
- 111 照明装置
- 112 レチクル駆動装置

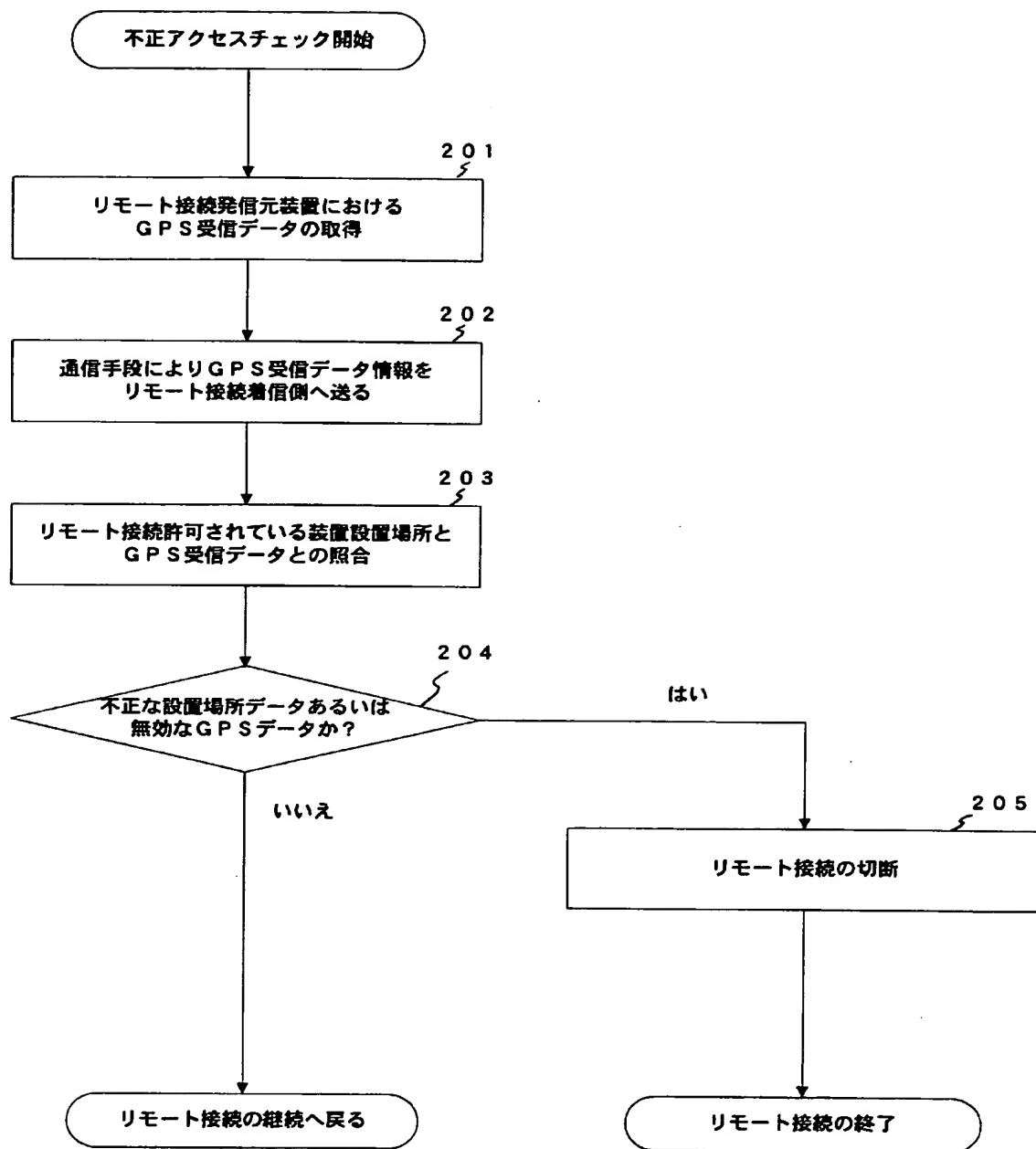
- 1 1 3 ステージ駆動装置
- 1 1 4 T V システム
- 1 1 5 周辺機器用バス
- 1 1 6 通信装置
- 1 1 7 通信網
- 1 5 0 サーバ機

【書類名】 図面

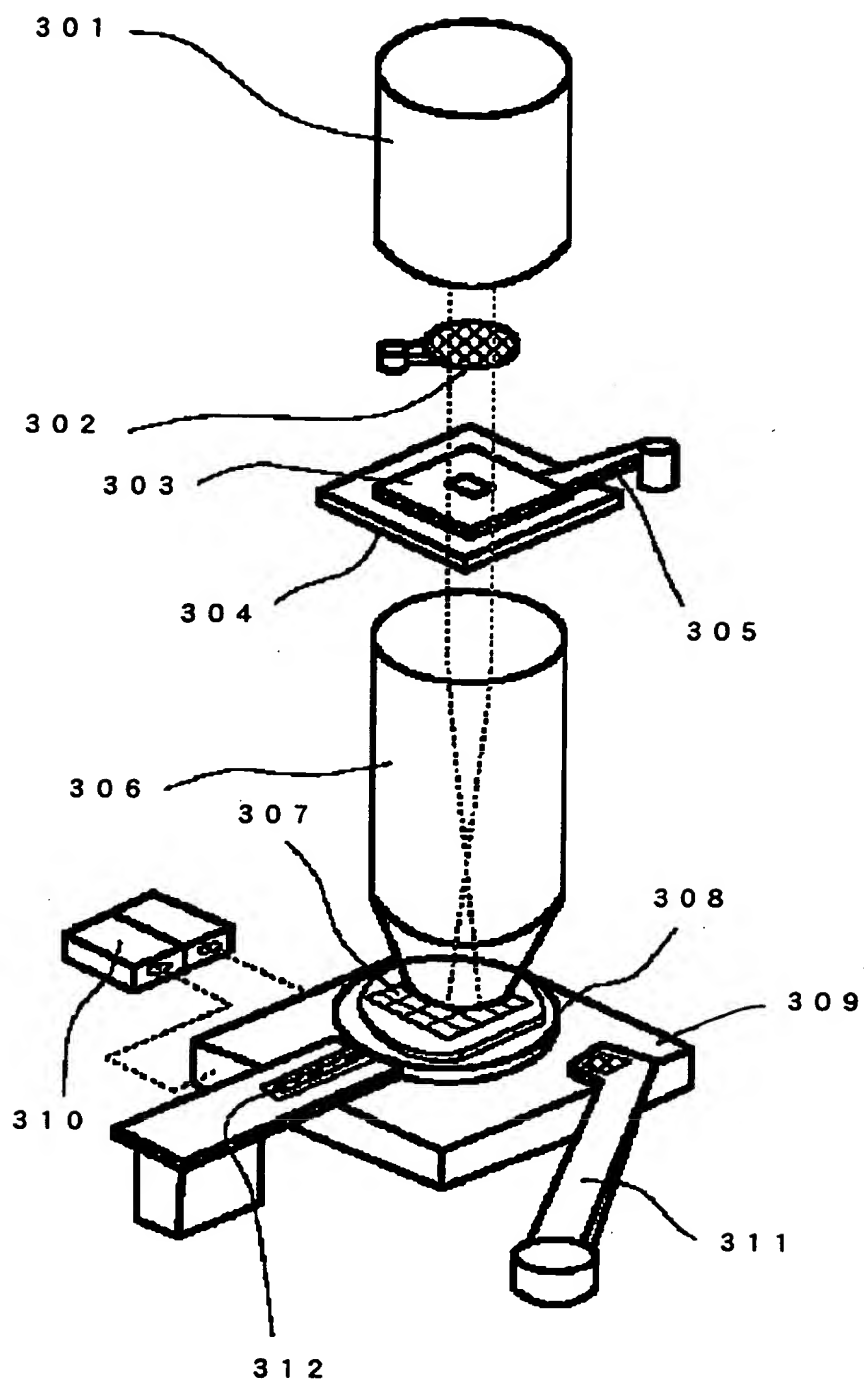
【図 1】



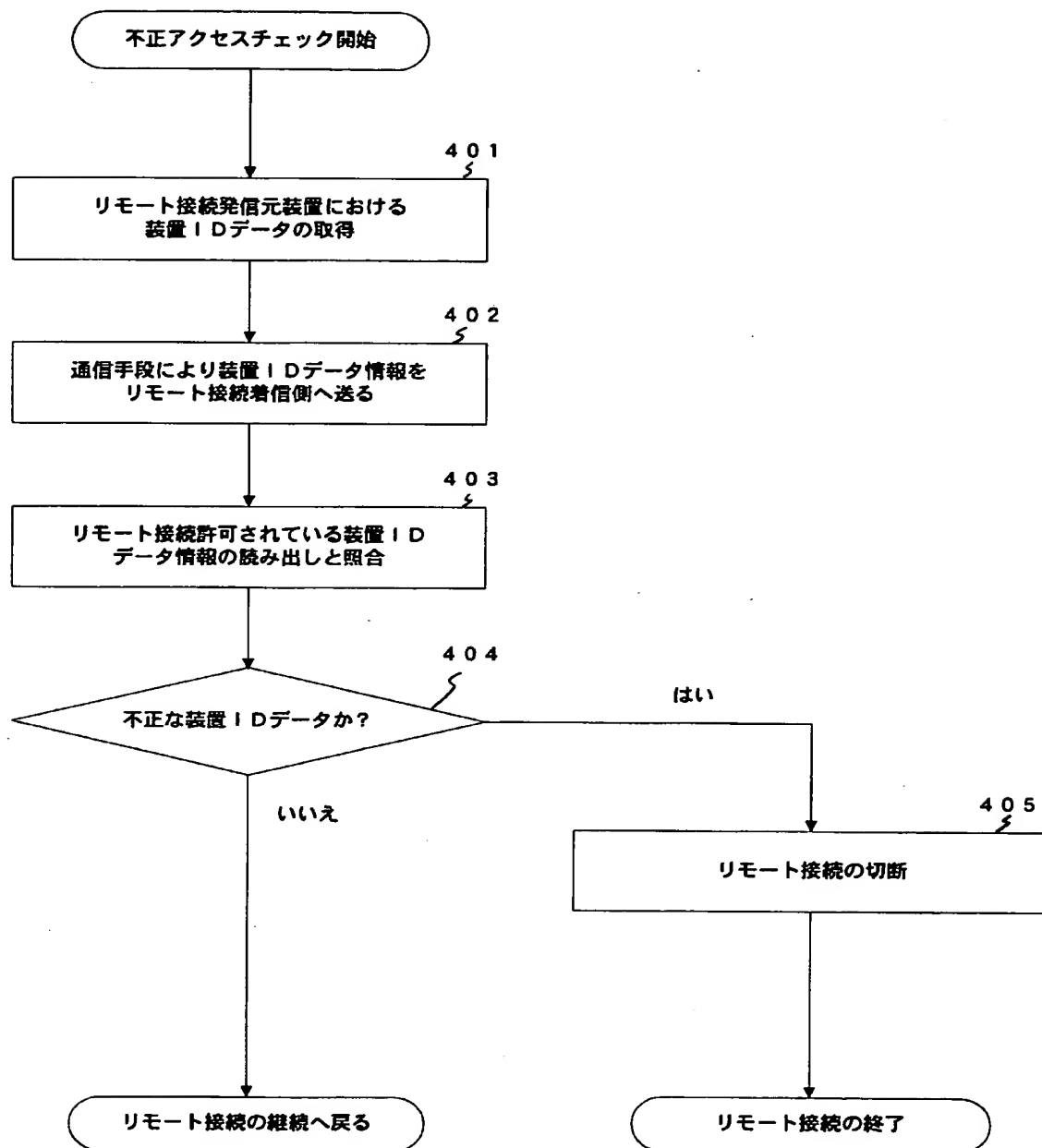
【図 2】



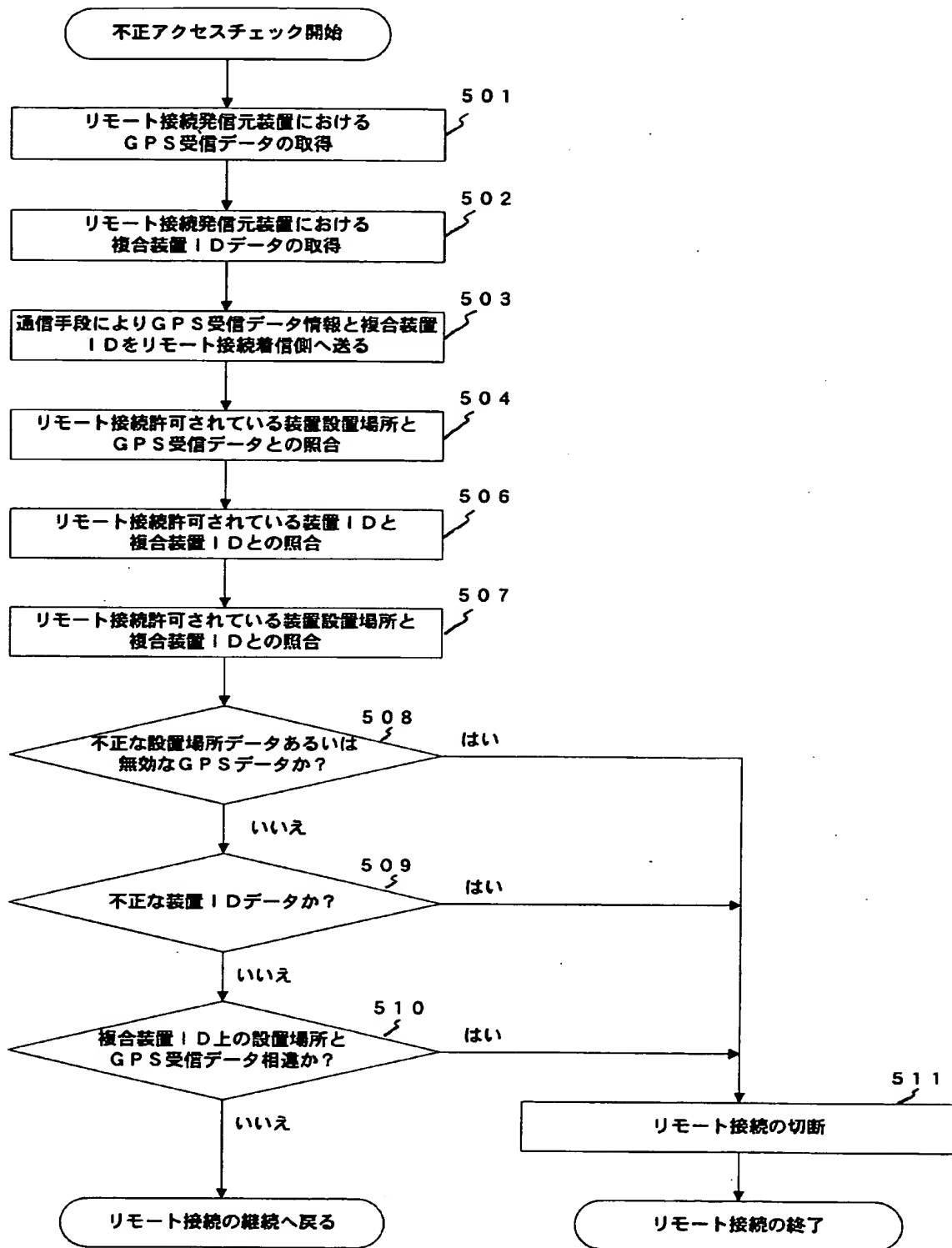
【図 3】



【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 不正なりモートアクセスを確実に防止できるようにする。

【解決手段】 半導体露光装置とサーバ機 1 5 0 等との間でのリモートアクセスが開始されると、半導体露光装置では、GPS受信機 1 0 8 により当該半導体露光装置が現在設置されている場所の緯度経度情報が取得されて、そのGPS受信データ（緯度経度情報）が通信インターフェース 1 0 9 及び通信装置 1 1 6 を介してサーバ機 1 5 0 等へ送出され、サーバ機 1 5 0 等では、受信したGPS受信データによる装置設置場所の緯度経度情報をリモートアクセスを許可すべきユーザ装置設置場所の緯度経度情報と比較・照合して、不正な設置場所データ、或いは改ざん、偽造による無効なGPS受信データであると判断した場合には、リモートアクセスを切断する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都大田区下丸子3丁目30番2号
氏 名	キヤノン株式会社